SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Judita Janković

PRSTENI POLINOMA I FORMALNIH REDOVA

Diplomski rad

Voditelj rada:
akademik Goran Muić

Zagreb, rujan 2018.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Sadržaj **iii**

Uvod **1**

1 Pregled rezultata iz teorije prstena **2**
1.1 Grupa 2
1.2 Prsten 7

2 Prsten polinoma i formalnih redova **21**
2.1 Prsten polinoma 21
2.2 Prsten formalnih redova 32

Bibliografija **38**

Uvod

Naslov ovog diplomskog rada zahtijeva pojašnjenje triju matematičkih pojmova – prstena, polinoma i formalnih redova. Za početak uvedimo pojam prstena. Još u prvom razredu osnovne škole susrećemo se sa prirodnim brojevima koje zbrajamo i množimo. Pritom podrazumijevamo da vrijede svojstva zatvorenosti, asocijativnosti, komutativnosti i postojanje neutralnog elementa. Nekoliko godina kasnije, u petom i šestom razredu, skup prirodnih brojeva proširujemo na skupove cijelih i racionalnih brojeva koji postojeću strukturu obogaćuju sa novim svojstvom – postojanjem inverznih elemenata. Tu se učenici također i po prvi puta susreću sa svojstvom distibutivnosti množenja prema zbrajanju. Dosad spomenuta svojstva dovoljna su za konstrukciju osnovne algebarske strukture kojom ćemo se baviti u ovom diplomskom radu - prstena. Definiciju, primjere i svojstva prstena dat ćemo u prvom poglavlju. Sljedeći pojam koji je potrebno pojasniti jesu polinomi. S najjednostavnijim oblicima polinoma susrećemo se u sedmom i osmom razredu. To su linearna i kvadratna funkcija, odnosno polinomi prvog i drugog stupnja jedne varijable. Polinomima n-tog stupnja jedne varijable upoznajemo se u prvom razredu srednje škole, gdje ih zbrajamo i množimo te pritom koristimo sva svojstva koja vrijede za strukturu prstena. Otuda dolazi poveznica između prstena i polinoma. Dakle, skup polinoma sa operacijama zbrajanja i množenja tvori prsten. Spomenimo još da se u četvrtom razredu obrađuju polinomi n-tog stupnja jedne varijable. Osim toga, tek se u visokoškolskom obrazovanju susrećemo s polinomima n-tog stupnja više varijabli. Na kraju preostaje pojasniti pojam formalnog reda i njegovu vezu sa središnjim pojmom ovog rada. Formalni redovi su "beskonačni polinomi" i sa njima se susrećemo tek na matematičkim fakultetima. Osim definicije formalnih redova pokazat ćemo da oni tvore strukturu prstena te ćemo iskazati neka njihova svojstva. Iako postoje formalni redovi n varijabli, u drugom poglavlju ovog rada mi ćemo se baviti formalnim redovima jedne varijable te pokazati povezanost sa polinomima jedne varijable.

Poglavlje 1

Pregled rezultata iz teorije prstena

U ovom poglavlju definirat ćemo osnovne pojmove vezane uz glavni termin ovog diplomskog rada - prstenove. Osim definicija navest ćemo i neke primjere definiranih pojmova. Kako je prsten građen od algebarski jednostavnije strukture - grupe, najprije ćemo definirati taj pojam.

1.1 Grupa

Definicija 1.1.1. Uređeni par $(G, \cdot)$, gdje je $\cdot : G \times G \to G$ binarna operacija, zove se **grupoid**.

Definicija 1.1.2. Grupoid u kojem vrijedi asocijativnost nazivamo **polugrupom**.

Definicija 1.1.3. Polugrupa koja ima neutralni element zove se **monoid**.

Definicija 1.1.4. Uređeni par $(G, \cdot)$, gdje je $\cdot : G \times G \to G$ binarna operacija, zove se **grupa** ako vrijede sjedeća svojstva:

(i) $(x \cdot y) \cdot z = x \cdot (y \cdot z), \qquad \forall x, y, z \in G$ (asocijativnost)

(ii) $(\exists e \in G) \quad e \cdot x = x \cdot e = x, \qquad \forall x \in G$ (neutralni element)

(iii) $(\forall x \in G)(\exists! x^{-1} \in G) \quad x \cdot x^{-1} = x^{-1} \cdot x = e$ (inverzni element)

Dakle, grupa je monoid u kojem svaki element ima svoj inverz.

Primjer 1.1.5. Grupa: Grupa permutacija skupa S. $\triangle$

Pokažimo da je $(Perm(S), \circ)$ grupa, pri čemu je $Perm(S) = \{f : S \to S \mid f \text{ bijekcija}\}$. Neka su $f, g \in Perm(S)$, odnosno f i g su bijekcije.

Zatvorenost: Želimo pokazati da je $f \circ g \in Perm(S)$, odnosno da je $f \circ g$ bijekcija (tj. injekcija i surjekcija).

Napomena 1.1.6. Pokažimo da općenito vrijedi da je kompozicija dviju bijekcija $f : B \to C, g : A \to B$ bijekcija. $\triangle$

- Injektivnost:
  Neka su x_1, x_2 takvi da $x_1 \neq x_2$. Tada je $g(x_1) \neq g(x_2)$ (jer je g injekcija). Slijedi $f(g(x_1)) \neq f(g(x_2))$ (jer je f injekcija). Dakle, $(f \circ g)(x_1) \neq (f \circ g)(x_2)$, odnosno $f \circ g$ je injekcija.

- Surjektivnost:
  Pokažimo da za surjekcije $f : B \to C$ i $g : A \to B$ vrijedi da je $f \circ g$ surjekcija.
  Zbog f je surjekcija vrijedi:
  $\forall z \in C \ \exists y \in B$ takav da je $f(y) = z$ $(\diamond)$
  i zbog g je surjekcija vrijedi:
  $\forall y \in B \ \exists x \in A$ takav da je $g(x) = y$ $(*)$.
  Dakle, zbog $(\diamond)$ vrijedi $\forall z \in C \ \exists y \in B$ te zbog $(*) \ \exists x \in A$ takav da je $g(x) = y$ te $f(y) = z$. Odnosno, $\forall z \in C \ \exists x \in A$ takav da $f(g(x)) = z$.
  Dakle, $f \circ g$ je surjekcija.

S obzirom da smo pokazali da je $f \circ g$ injekcija i surjekcija, slijedi da je bijekcija. Odnosno, $f \circ g$ je iz $Perm(S)$.

Asocijativnost: Pokažimo da za funkcije $f : C \to D, g : B \to C, h : A \to B$ vrijedi: $(f \circ g) \circ h = f \circ (g \circ h)$.
Za svaki $x \in A$ vrijedi:
$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$
$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$

Neutralni element: Pokažimo da za funkciju $id : S \to S,\ id(x) = x$ vrijedi $f \circ id = id \circ f = f$. Za svaki $x \in S$ vrijedi:
$(f \circ id)(x) = f(id(x)) = f(x)$
$(id \circ f)(x) = id(f(x)) = f(x)$

Inverzni element: S obzirom da je f bijekcija, za nju postoji funkcija $f^{-1} : S \to S$ takva da $f \circ f^{-1} = f^{-1} \circ f = id$.

Definicija 1.1.7. Ako u grupi vrijedi svojstvo komutativnosti, to jest

$$x \cdot y = y \cdot x, \quad \text{za sve} \quad x, y \in G$$

kažemo da je G **komutativna (Abelova) grupa**.

Primjer 1.1.8. Komutativna grupa: Skup svih matrica $(m \times n)$ nad skupom cijelih, racionalnih, realnih, kompleksnih brojeva. △

Pokažimo da je $(M_{3\times 2}(\mathbb{R}), +)$ Abelova grupa.

Zatvorenost:
Neka je $M_{3\times 2}(\mathbb{R}) = \left\{ \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix} : a_{ij} \in \mathbb{R} \right\}$

i neka je $x = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix}$ i $y = \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \\ b_{20} & b_{21} \end{pmatrix}$.

Pokažimo da je $x + y \in M_{3\times 2}(\mathbb{R})$.

$$x + y = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix} + \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \\ b_{20} & b_{21} \end{pmatrix} = \begin{pmatrix} a_{00}+b_{00} & a_{01}+b_{01} \\ a_{10}+b_{10} & a_{11}+b_{11} \\ a_{20}+b_{20} & a_{21}+b_{21} \end{pmatrix}$$

Na svakoj koordinati nalazi se zbroj dva realna broja (a skup $\mathbb{R}$ je grupa sa zbrajanjem) pa slijedi da je zbroj iz $M_{3\times 2}(\mathbb{R})$. Dakle, $M_{3\times 2}(\mathbb{R})$ je grupoid.

Asocijativnost:

$$\begin{aligned}
(x+y)+z &= \left(\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix} + \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \\ b_{20} & b_{21} \end{pmatrix}\right) + \begin{pmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \\ c_{20} & c_{21} \end{pmatrix} \\
&= \begin{pmatrix} a_{00}+b_{00} & a_{01}+b_{01} \\ a_{10}+b_{10} & a_{11}+b_{11} \\ a_{20}+b_{20} & a_{21}+b_{21} \end{pmatrix} + \begin{pmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \\ c_{20} & c_{21} \end{pmatrix} \\
&= \begin{pmatrix} (a_{00}+b_{00})+c_{00} & (a_{01}+b_{01})+c_{01} \\ (a_{10}+b_{10})+c_{10} & (a_{11}+b_{11})+c_{11} \\ (a_{20}+b_{20})+c_{20} & (a_{21}+b_{21})+c_{21} \end{pmatrix} \\
&\overset{\substack{\text{(asoc.}\\ \text{u } \mathbb{R})}}{=} \begin{pmatrix} a_{00}+(b_{00}+c_{00}) & a_{01}+(b_{01}+c_{01}) \\ a_{10}+(b_{10}+c_{10}) & a_{11}+(b_{11}+c_{11}) \\ a_{20}+(b_{20}+c_{20}) & a_{21}+(b_{21}+c_{21}) \end{pmatrix} \\
&= \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix} + \begin{pmatrix} b_{00}+c_{00} & b_{01}+c_{01} \\ b_{10}+c_{10} & b_{11}+c_{11} \\ b_{20}+c_{20} & b_{21}+c_{21} \end{pmatrix} \\
&= \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix} + \left(\begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \\ b_{20} & b_{21} \end{pmatrix} + \begin{pmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \\ c_{20} & c_{21} \end{pmatrix}\right) = x + (y+z)
\end{aligned}$$

$M_{3\times 2}(\mathbb{R})$ je polugrupa.

Neutralni element:

Pokažimo da je $e = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$ takav da je $x + e = x = e + x$.

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{00}+0 & a_{01}+0 \\ a_{10}+0 & a_{11}+0 \\ a_{20}+0 & a_{21}+0 \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix}$$
$$= \begin{pmatrix} 0+a_{00} & 0+a_{01} \\ 0+a_{10} & 0+a_{11} \\ 0+a_{20} & 0+a_{21} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix}$$

$M_{3\times 2}(\mathbb{R})$ je monoid.

Inverzni element:

Pokažimo da je $-x = \begin{pmatrix} -a_{00} & -a_{01} \\ -a_{10} & -a_{11} \\ -a_{20} & -a_{21} \end{pmatrix}$ takav da je $x + (-x) = e = (-x) + x$.

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix} + \begin{pmatrix} -a_{00} & -a_{01} \\ -a_{10} & -a_{11} \\ -a_{20} & -a_{21} \end{pmatrix} = \begin{pmatrix} a_{00}+(-a_{00}) & a_{01}+(-a_{01}) \\ a_{10}+(-a_{10}) & a_{11}+(-a_{11}) \\ a_{20}+(-a_{20}) & a_{21}+(-a_{21}) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} (-a_{00})+a_{00} & (-a_{01})+a_{01} \\ (-a_{10})+a_{10} & (-a_{11})+a_{11} \\ (-a_{20})+a_{20} & (-a_{21})+a_{21} \end{pmatrix} = \begin{pmatrix} -a_{00} & -a_{01} \\ -a_{10} & -a_{11} \\ -a_{20} & -a_{21} \end{pmatrix} + \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix}$$

$M_{3\times 2}(\mathbb{R})$ je grupa.

Komutativnost:

Pokažimo da je $x + y = y + x$.

$$x+y=\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix}+\begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \\ b_{20} & b_{21} \end{pmatrix}=\begin{pmatrix} a_{00}+b_{00} & a_{01}+b_{01} \\ a_{10}+b_{10} & a_{11}+b_{11} \\ a_{20}+b_{20} & a_{21}+b_{21} \end{pmatrix}$$
$$\overset{\text{(komut u } \mathbb{R})}{=}\begin{pmatrix} b_{00}+a_{00} & b_{01}+a_{01} \\ b_{10}+a_{10} & b_{11}+a_{11} \\ b_{20}+a_{20} & b_{21}+a_{21} \end{pmatrix}=\begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \\ b_{20} & b_{21} \end{pmatrix}+\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \\ a_{20} & a_{21} \end{pmatrix}=y+x$$

$M_{3\times 2}(\mathbb{R})$ je Abelova grupa.

Analogno bismo dokazali da je $(M_{m,n}(F),+)$ Abelova grupa.

S obzirom da smo definirali grupu, sada možemo definirati prsten.

1.2 Prsten

Definicija 1.2.1. Uređena trojka $(R,+,\cdot)$ zove se **prsten** ako za operacije zbrajanja $+ : R\times R\to R$ i množenja $\cdot : R\times R\to R$ vrijedi:

(i) $(R,+)$ je komutativna grupa

(ii) $(R,\cdot)$ je polugrupa

(iii) distributivnost množenja prema zbrajanju, to jest:
$x\cdot(y+z)=x\cdot y+x\cdot z$
$(x+y)\cdot z=x\cdot z+y\cdot z$

za svaki izbor $x,y,z\in R$.

Iz definicije možemo zaključiti da prsten nije struktura koja je inducirana s dvije neovisne operacije, već da te operacije moraju biti međusobno usklađene, odnosno povezane zakonom distribucije.

Primjer 1.2.2. Prsten:

(i) Skup svih polinoma čiji je slobodni član jednak nuli.

(ii) Za svaki $n \in \mathbb{N}$, skup $n\mathbb{Z}$.

△

Definicija 1.2.3. Prsten R je **komutativan prsten** ako je

$$x \cdot y = y \cdot x, \quad \text{za sve} \quad x, y \in R.$$

Definicija 1.2.4. Ako postoji **jedinični element** ili kraće **jedinica**, $1 = 1_R \in R$ takav da je

$$1 \cdot x = x \cdot 1 = x, \qquad \forall x \in R$$

onda kažemo da je R **prsten s jedinicom**.

Primjer 1.2.5. Prsten s jedinicom: Skup svih kvadratnih matrica reda n nad skupovima realnih i kompleksnih brojeva. △

Pokažimo da je $(M_2(\mathbb{R}), +, \cdot)$ prsten.

S obzirom da je $(M_{m\times n}(\mathbb{R}), +)$ komutativna grupa $\forall m, n$ slijedi da je $(M_2(\mathbb{R}), +)$ komutativna grupa. Stoga još trebamo dokazati da je $(M_2(\mathbb{R}), \cdot)$ polugrupa te da vrijedi lijeva i desna distrubutivnost.

Pokažimo da je $(M_2(\mathbb{R}), \cdot)$ polugrupa.

$$xy = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$$

Na svakoj koordinati je realan broj pa je dobivena matrica iz $M_2(\mathbb{R})$. Slijedi, $M_2(\mathbb{R})$ je grupoid.

$$
\begin{aligned}
(xy)z &= \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right)\begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
&= \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}\begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
&= \begin{pmatrix} (ae+bg)i+(af+bh)k & (ae+bg)j+(af+bh)l \\ (ce+dg)i+(cf+dh)k & (ce+dg)j+(cf+dh)l \end{pmatrix} \\
&= \begin{pmatrix} aei+bgi+afk+bhk & aej+bgj+afl+bhl \\ cei+dgi+cfk+dhk & cej+dgj+cfl+dhl \end{pmatrix} \\
&\overset{\substack{\text{(komut. zbroja} \\ \text{i distr.} \\ \text{u } \mathbb{R})}}{=} \begin{pmatrix} a(ei+fk)+b(gi+hk) & a(ej+fl)+b(gj+hl) \\ c(ei+fk)+d(gi+hk) & c(ej+fl)+d(gj+hl) \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} i & j \\ k & l \end{pmatrix}\right) = x(yz)
\end{aligned}
$$

S obzirom da vrijedi asocijativnost, $M_2(\mathbb{R})$ je polugrupa.

Pokažimo još da vrijedi lijeva i desna disributivnost:

$$\begin{aligned}
x(y+z) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \left(\begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} i & j \\ k & l \end{pmatrix} \right) \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e+i & f+j \\ g+k & h+l \end{pmatrix} \\
&= \begin{pmatrix} a(e+i)+b(g+k) & a(f+j)+b(h+l) \\ c(e+i)+d(g+k) & c(f+j)+d(h+l) \end{pmatrix} \\
&= \begin{pmatrix} ae+ai+bg+bk & af+aj+bh+bl \\ ce+ci+dg+dk & cf+cj+dh+dl \end{pmatrix} \\
&\overset{\text{(komut. zbroja u } \mathbb{R})}{=} \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} + \begin{pmatrix} ai+bk & aj+bl \\ ci+dk & cj+dl \end{pmatrix} = xy+xz
\end{aligned}$$

Analogno bi se pokazalo da je $(x+y)z = xz+yz$.

U ovom radu susretat ćemo se i s komutativnim prstenom s jedinicom. On se definira pomoću prethodne dvije definicije.

Primjer 1.2.6. Komutativni prsten s jedinicom:

(i) Skupovi cijelih, racionalnih, realnih i kompleksnih brojeva sa standardnim operacijama zbrajanja i množenja.

(ii) Za svaki $n \in \mathbb{N}$ skup $\mathbb{Z}_n$ uz zbrajanje i množenje $mod \ \ n$.

△

Pokažimo da je $(\mathbb{Z}_n, +_n, \cdot_n)$ komutativni prsten s jedinicom.

$(\mathbb{Z}_n, +_n)$ je komutativna grupa:

Napomena 1.2.7. Za $z \in \mathbb{Z}_n$ vrijedi $z = z \ mod \ n$. △

Zatvorenost:
$x +_n y = (x + y) mod\ n$. Prema definiciji dijeljenja s ostatkom, dobiveni izraz je element skupa $\mathbb{Z}_n$.

Asocijativnost:

$$\begin{aligned}
(x +_n y) +_n z &= (((x + y) mod\ n) + z) mod\ n \\
&\overset{\text{(Nap. 1.2.7.)}}{=} (((x + y) mod\ n) + z\ mod\ n) mod\ n \\
&\overset{\text{(svojstvo mod. aritm.)}}{=} (x + y) + z) mod\ n. \\
&\overset{\text{(asoc. u } \mathbb{Z})}{=} (x + (y + z)) mod\ n. \\
&\overset{\text{(svojstvo mod. aritm.)}}{=} (x\ mod\ n + (y + z) mod\ n) mod\ n \\
&\overset{\text{(Nap. 1.2.7.)}}{=} (x + (y + z) mod\ n) mod\ n = x +_n (y +_n z)
\end{aligned}$$

Komutativnost:

$$x +_n y = (x + y) mod\ n \overset{\text{(komut. u } \mathbb{Z})}{=} (y + x) mod\ n = y +_n x$$

Neutralni element:
Pokažimo da je 0 neutralni element.
Zbog komutativnosti $\mathbb{Z}_n$ dovoljno je pokazati da je $x +_n 0 = x$.
$x +_n 0 = (x + 0) mod\ n = x\ mod\ n$. Zbog $x \in \mathbb{Z}_n$ slijedi $x\ mod\ n = x$.

Inverzni element:
Pokažimo da je $y = n - x$ inverz od x.
$x +_n y = (x + y) mod\ n = (x + (n - x)) mod\ n = n\ mod\ n = 0$

Pokažimo da je $(\mathbb{Z}_n, \cdot_n)$ komutativni monoid.

Zatvorenost:
$x \cdot_n y = (x \cdot y) mod\ n$. Prema definiciji dijeljenja s ostatkom, dobiveni izraz je element skupa $\mathbb{Z}_n$.

Asocijativnost:

$$\begin{aligned}
(x \cdot_n y) \cdot_n z &= (((xy) mod\ n)z) mod\ n \\
&\overset{\text{(Nap. 1.2.7.)}}{=} ((xy) mod\ n)z\ \ mod\ n) mod\ n \\
&\overset{\text{(svojstvo mod. aritm.)}}{=} ((xy)z) mod\ n \\
&\overset{\text{(asoc. u } \mathbb{Z})}{=} (x(yz)) mod\ n \\
&\overset{\text{(svojstvo mod. aritm.)}}{=} (x\ mod\ n\ \ (yz) mod\ n) mod\ n \\
&\overset{\text{(Nap. 1.2.7.)}}{=} (x(yz) mod\ n) mod\ n = x \cdot_n (y \cdot_n z)
\end{aligned}$$

Neutralni element:
$x \cdot_n 1 = (x \cdot 1) mod\ n = x\ \ mod\ n = x = x\ \ mod\ n = (1 \cdot x) mod\ n = 1 \cdot_n x$

Komutativnost:

$$x \cdot_n y = (xy) mod\ n \overset{\text{(komut. u } \mathbb{Z})}{=} (yx) mod\ n = y \cdot_n x$$

Distributivnost:

$$
\begin{aligned}
& x \cdot_n (y +_n z) \\
&= (x((y+z) mod\ n)) mod\ n \\
&\text{(Nap. 1.2.7.)} \\
&= (x\ mod\ n((y+z) mod\ n)) mod\ n \\
&\text{(svojstvo mod. aritm.)} \\
&= (x(y+z)) mod\ n \\
&\text{(distr. u } \mathbb{Z}\text{)} \\
&= (xy + xz) mod\ n \\
&\text{(svojstvo mod. aritm.)} \\
&= ((xy) mod\ n + (xz) mod\ n) mod\ n \\
&= (x \cdot_n y) +_n (x \cdot_n z)
\end{aligned}
$$

$$
\begin{aligned}
& (x +_n y) \cdot_n z \\
&= ((x+y) mod\ n)z) mod\ n \\
&\text{(Nap. 1.2.7.)} \\
&= ((x+y) mod\ n)z\ mod\ n) mod\ n \\
&\text{(svojstvo mod. aritm.)} \\
&= ((x+y)z) mod\ n \\
&\text{(distr. u } \mathbb{Z}\text{)} \\
&= (xz + yz) mod\ n \\
&\text{(svojstvo mod. aritm.)} \\
&= ((xz) mod\ n + (yz) mod\ n) mod\ n \\
&= (x \cdot_n z) +_n (y \cdot_n z)
\end{aligned}
$$

Nadalje, definirat ćemo podstrukturu prstena:

Definicija 1.2.8. Neka je R prsten, a $S \subseteq R$ njegov neprazni podskup. Kažemo da je S **potprsten** od R ako je S i sam prsten u odnosu na binarne operacije definirane na R.

Drugim riječima, S je potprsten od R ako vrijede sljedeći uvjeti:

(i) $(\forall x, y \in S) : x - y \in S$ (to jest $(S, +)$ je grupa)

(ii) $(\forall x, y \in S) : x \cdot y \in S$ (to jest $(S, \cdot)$ je grupoid).

Činjenicu da je S potprsten od R označit ćemo sa $S \leq R$.

Primjer 1.2.9. Potprsten:

(i) $\mathbb{Z}$ je potprsten od $\mathbb{Q}$, $\mathbb{Q}$ je potprsten od $\mathbb{R}$, $\mathbb{R}$ je potprsten od $\mathbb{C}$.

(ii) Za svaki $n \in \mathbb{N}, n\mathbb{Z} \subseteq \mathbb{Z}$ je potprsten od $\mathbb{Z}$.

△

Pokažimo da je $\forall n \in \mathbb{N}, n\mathbb{Z} \subseteq \mathbb{Z}$ potprsten od $\mathbb{Z}$.
Neka su $x, y \in n\mathbb{Z}$ takvi da $x = nz$ i $y = nt$, $z, t \in \mathbb{Z}$.
Tada je:

$$x - y = nz - nt \overset{\text{u } \mathbb{Z})}{\underset{\text{(distr.}}{=}} n(z - t) \in n\mathbb{Z}$$

$$x \cdot y = (nz)(nt) \overset{\text{u } \mathbb{Z})}{\underset{\text{(asoc.}}{=}} n(znt) \in n\mathbb{Z}$$

Definirajmo sada još neke pojmove koji će nam biti važni za razumijevanje tematike ovog rada. Za početak, prisjetimo se da kod poznatijih prstenova (poput $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$) izraz $ab = 0$ povlači da je bar jedan od faktora jednak nuli. U općim prstenovima to ne mora biti istina, stoga se javila potreba za sljedećom definicijom:

Definicija 1.2.10. Neka je R prsten, $0 \neq \lambda \in R$ (odnosno $0 \neq \rho \in R$) te neka je $0 \neq x \in R$ takav da je $\lambda x = 0$ (to jest $x\rho = 0$). λ (odnosno ρ) zove se **lijevi** (to jest **desni**) **djelitelj nule**.

Primjer 1.2.11. U prstenu $(\mathbb{Z}_8, +_8, \cdot_8)$ vrijedi: $2 \neq 0, 4 \neq 0$, ali $2 \cdot_8 4 = 0$.
Također, u svakom prstenu $\mathbb{Z}_m$, gdje je m složen broj postoje djelitelji nule. △

S obzirom da smo definirali pojam djelitelja nule, možemo dati sljedeću definiciju:

Definicija 1.2.12. R je **integralna domena**, ili kraće **domena**, ako nema ni lijevih ni desnih djelitelja nule.

Primjer 1.2.13. Integralna domena:

(i) Prsten cijelih, racionalnih, realnih i kompleksnih brojeva.

(ii) Prsten $\mathbb{Z}_m$, gdje je m prost broj.

△

Definicija 1.2.14. Element $\omega \in R$, gdje je R prsten s jedinicom, je **invertibilan** ako $\exists \omega' \in R$ takav da je $\omega \cdot \omega' = \omega' \cdot \omega = 1$. Grupa invertibilnih elemenata u R označava se sa $R^\times$.

Primjer 1.2.15. Invertibilan element:

(i) U prstenu cijelih brojeva invertibilni elementi su 1 i -1.

(ii) U prstenu racionalnih brojeva invertibilni elementi su svi osim 0.

△

Definicija 1.2.16. Neka je R prsten. Podskup $I \subseteq R$ je **lijevi** (to jest **desni**)**ideal** u R, ako su ispunjeni uvjeti:

(i) I je potprsten od R

(ii) Za sve $r \in R$ i $x \in I$ je $r \cdot x \in I$ (to jest $x \cdot r \in I$).
Podskup $I \subseteq R$ je **dvostrani ideal** ili **ideal** ako je on istovremeno i lijevi i desni ideal.

Činjenicu da je I ideal u prstenu R označavamo sa $I \trianglelefteq R$.

Primjer 1.2.17. Ideal: U prstenu svih polinoma s dvije varijable, potprsten polinoma s dvije varijable bez slobodnog člana. △

Definicija 1.2.18. Neka je R prsten. **Centar** od R je skup

$$C = \{c \in R : cr = rc, \forall r \in R\}.$$

Teorem 1.2.19. Neka je R prsten s jedinicom i neka je a iz centra od R. Tada vrijedi:

$$Ra = (a) = aR.$$

Ideal (a) nazivamo **glavnim idealom**.

Primjer 1.2.20. Glavni ideal:

(i) Svaki ideal oblika $n\mathbb{Z}, n \in \mathbb{N}$ je glavni.

(ii) U prstenu polinoma s jednom varijablom, potprsten polinoma s jednom varijablom bez slobodnog člana je glavni ideal (x).

△

Definicija 1.2.21. Prsten R je **prsten glavnih ideala** ako je svaki ideal u R glavni ideal.

Primjer 1.2.22. Prsten glavnih ideala: prsten cijelih brojeva.

△

Definicija 1.2.23. Neka je R prsten. Kažemo da je M **maksimalni ideal** u R, ako vrijedi:

- $M \neq R$
- Ako je I ideal od R takav da je $M \subseteq I \subset R$, onda je $M = I$.

Drugim riječima, ideal $M \trianglelefteq R$ prstena R je maksimalan, ako su jedini ideali koji sadrže M, sam M i čitav R.

Primjer 1.2.24. Maksimalni ideal: U prstenu cijelih brojeva, maksimalni ideali su svi $n\mathbb{Z}$, takvi da je n prost broj. △

Definicija 1.2.25. Komutativni prsten s jedinicom R je **lokalni prsten**, ako sadrži jedinstveni maksimalni ideal u R.

Primjer 1.2.26. Lokalni prsten:

(i) Sva polja su lokalni prsteni.

(ii) Prsten racionalnih brojeva s neparnim nazivnikom.

△

Definicija 1.2.27. Element $c \in R$ je **ireducibilan** ako vrijede sljedeća svojstva:

(i) $0 \neq c \notin R^\times$

(ii) Ako je $c = ab$, onda je ili $a \in R^\times$ ili $b \in R^\times$.

Drugim riječima, element je ireducibilan ako je to ne-nul neinvertibilan element koji se ne može napisati kao produkt dva neinvertibilna elementa.

Primjer 1.2.28. Ireducibilni element:

(i) U prstenu cijelih brojeva n je ireducibilan, ako i samo ako je n prost.

(ii) U prstenu oblika $\mathbb{Z}_n$ pri čemu je n prost nema ireducibilnih elemenata.

△

Nadalje, definirat ćemo preslikavanja između prstenova koja poštuju dane strukture i pomoću kojih se te strukture (prstenovi) mogu uspoređivati.

Definicija 1.2.29. Neka su R i S dva prstena. Preslikavanje $f : R \to S$ je **homomorfizam** prstena ako za svaki izbor $x, y \in R$ vrijedi

(i) $f(x + y) = f(x) + f(y)$,

(ii) $f(x \cdot y) = f(x) \cdot f(y)$

to jest, ako f komutira s obje binarne operacije.

Primijetimo da za R i S prstene s jedinicom mora vrijediti i $f(1_R) = 1_S$.

Postoje i specijalni homomorfizmi prstenova. Definirajmo neke od njih:
Homomorfizam f koji je i injekcija naziva se **monomorfizam**.
Homomorfizam f koji je i surjekcija naziva se **epimorfizam**.
Homomorfizam f koji je i bijekcija naziva se **izomorfizam**.

Sljedeće definicije govore o strukturama koje su bogatije od prstena, a koje ćemo također proučavati.

Definicija 1.2.30. Prsten R je **tijelo**, ili **prsten s dijeljenjem**, ako je svaki ne-nul element u R invertibilan; to jest ukoliko je $R^\times = R\backslash\{0\}$.
Komutativno tijelo zove se **polje**.

Primjer 1.2.31. Tijelo:

(i) Skup regularnih matrica.

(ii) Kvaternioni.

Polje:

(i) Skupovi racionalnih, realnih i kompleksnih brojeva uz standardne operacije.

(ii) Prsten $(\mathbb{Z}_n, +_n, \cdot_n)$ za n prost broj.

△

Pokažimo da je $(\mathbb{Z}_n, +_n, \cdot_n)$ polje za n prost broj.
Ranije smo pokazali da je $(\mathbb{Z}_n, +_n, \cdot_n)$ komutativni prsten s jedinicom za svaki n.
Preostaje još pokazati da je svaki $x \in \mathbb{Z}_n$ invertibilan.

Inverzni element:
Zbog komutativnosti s obzirom na množenje vrijedi da su lijevi i desni inverz jednaki.

Lema 1.2.32. U svakom $\mathbb{Z}_n$ invertibilni elementi su oni koji su relativno prosti s n.

Dokaz.

$$\begin{aligned}
&\exists y \in \mathbb{Z}_n \text{ takav da je } y \cdot_n x = 1\\
\Longleftrightarrow &\exists y \in \mathbb{Z} \text{ takav da je } (y \ mod \ n) \cdot_n x = 1\\
\Longleftrightarrow &\exists y \in \mathbb{Z} \text{ takav da je } (y \ mod \ n \cdot x) mod \ n = 1\\
\Longleftrightarrow &\exists y \in \mathbb{Z} \text{ takav da je } (y \cdot x) mod \ n = 1\\
\Longleftrightarrow &\exists y, b \in \mathbb{Z} \text{ takvi da je } yx = bn + 1\\
\Longleftrightarrow &\exists y, b \in \mathbb{Z} \text{ takvi da je } yx - bn = 1\\
\Longleftrightarrow &M(x, n) = 1
\end{aligned}$$

■

S obzirom da je n prosti, tvrdnja vrijedi za svaki $0 \neq x \in \mathbb{Z}_n$.

Napomena 1.2.33. Brojevi a i b dobivaju se Euklidovim algoritmom. $\triangle$

Poglavlje 2

Prsten polinoma i formalnih redova

2.1 Prsten polinoma

U drugom poglavlju prisjetit ćemo se definicije polinoma iz srednje škole te kako je definirano njihovo zbrajanje i množenje. Nakon toga bavit ćemo se teoremima vezanim uz prsten polinoma jedne varijable koji ćemo zatim proširiti na prsten polinoma n varijabli. Na kraju poglavlja napravit ćemo mali uvod o prstenu formalnih redova jedne varijable iznad prstena R.

U srednjoj školi izraz oblika $f(x) = a_0 + a_1x + ... + a_nx^n$ gdje su $a_0, a_1, ..., a_n \in \mathbb{R}$, $a_n \neq 0, n \in \mathbb{N}$ nazivamo **polinomom n-tog stupnja** u varijabli x. Elemente $a_i, i = 0, ..., n$ nazivamo koeficijentima polinoma f, gdje a_n nazivamo vodećim, a a_0 slobodnim koeficijentom od f. Nadalje, polinom za koji vrijedi da je $a_n = 1$ nazivamo normiranim polinomom, a polinom u kojem za svaki $x \in \mathbb{R}$ vrijedi $f(x) = 0$ nazivamo nulpolinomom. Drugačije polinom možemo zapisati kao $f(x) = \sum_{i=0}^{n} a_i x^i$. Operacije zbrajanja i množenja polinoma $f(x) = \sum_{i=0}^{n} a_i x^i$ i $g(x) = \sum_{i=0}^{m} b_i x^i$ definirane su na sljedeći način:

- **zbroj polinoma** $f(x) + g(x) = \sum_{i=0}^{max\{n,m\}} (a_i + b_i)x^i$
- **produkt polinoma** $f(x) \cdot g(x) = \sum_{i=0}^{n+m} c_i x^i$ gdje je $c_i = a_0b_i + a_1b_{i-1} + ... + a_ib_0$.

S obzirom da se u srednjoj školi ne definira polinom više varijabli, njega ćemo definirati:

Definicija 2.1.1. Preslikavanje $f : R^n \to R$ definirano formulom:

$$f(x_1, ..., x_n) = f_0(x_1, ..., x_{n-1}) + f_1(x_1, ..., x_{n-1})x_n + f_1(x_1, ..., x_{n-1})x_n^2 + ... + f_n(x_1, ..., x_{n-1})x_n^n,$$

$$(x_1, ..., x_n) \in R^n$$

gdje su $f_0, f_1, ..., f_n$ polinomi $(n-1)$ varijabli zove se **polinom n varijabli**.

Zbrajanje i množenje polinoma n varijabli analogno je zbrajanju i množenju polinoma jedne varijable.

Slijedi teorem koji pokazuje kako je u prstenu polinoma jedne varijable definirano zbrajanje i množenje polinoma. Također, teorem govori i o odnosu između prstena polinoma i prstena iz kojeg potječu koeficijenti tog polinoma.

Teorem 2.1.2. Neka je R prsten i neka $R[x]$ označava skup svih nizova elemenata prstena R $(a_0, a_1, a_2, ...)$ takvih da je $a_i = 0$ za sve osim za konačno mnogo članova niza. Tada vrijedi:

(i) $R[x]$ je prsten sa zbrajanjem

$$(a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...)$$

i množenjem

$$(a_0, a_1, ...) \cdot (b_0, b_1, ...) = (c_0, c_1, ...)$$

gdje je

$$\begin{aligned} c_n &= \sum_{i=0}^{n} a_{n-i} b_i \\ &= a_n b_0 + a_{n-1} b_1 + ... + a_1 b_{n-1} + a_0 b_n \\ &= \sum_{k+j=n} a_k b_j. \end{aligned}$$

(ii) Ako je R komutativni prsten (analogno: prsten s jedinicom ili prsten bez djelitelja nule ili integralna domena), onda je i $R[x]$.

(iii) Funkcija $R \to R[x]$ zadana preslikavanjem $r \mapsto (r, 0, 0, ...)$ je monomorfizam prstena.

Dokaz. Neka je $a = (a_0, a_1, ...)$, $b = (b_0, b_1, ...)$ te $c = (c_0, c_1, ...)$.

(i) Pokažimo najprije da je $(R, +)$ komutativna grupa:

Grupoid:

$a + b = (a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...)$
S obzirom da se na svakoj koordinati nalazi zbroj elemenata iz prstena R te za samo konačno mnogo indeksa i, j vrijedi da su a_i i b_j različiti od 0, vrijedi da je $a + b$ niz elemenata iz R koji su različiti od nula na samo konačno mnogo koordinata.

Polugrupa:

$$\begin{aligned}(a + b) + c &= ((a_0, a_1, ...) + (b_0, b_1, ...)) + (c_0, c_1, ...) \\ &= (a_0 + b_0, a_1 + b_1, ...) + (c_0, c_1, ...) \\ &= ((a_0 + b_0) + c_0, (a_1 + b_1) + c_1, ...)\end{aligned}$$

$$\begin{aligned}a + (b + c) &= (a_0, a_1, ...) + ((b_0, b_1, ...) + (c_0, c_1, ...)) \\ &= (a_0, a_1, ...) + (b_0 + c_0, b_1 + c_1, ...) \\ &= (a_0 + (b_0 + c_0), a_1 + (b_1 + c_1), ...)\end{aligned}$$

Zbog asocijativnosti elemenata iz prstena R vrijedi da su dobiveni izrazi jednaki.

Monoid:

$$a + e = (a_0, a_1, ...) + (0, 0, ...) = (a_0 + 0, a_1 + 0, ...) = (a_0, a_1, ...)$$

$$e + a = (0, 0, ...) + (a_0, a_1, ...) = (0 + a_0, 0 + a_1, ...) = (a_0, a_1, ...)$$

Grupa:

$$a+(-a) = (a_0, a_1, ...)+(-a_0, -a_1, ...) = (a_0+(-a_0), a_1+(-a_1), ...) = (0, 0, ...) = e$$

$$(-a)+a = (-a_0, -a_1, ...)+(a_0, a_1, ...) = (-a_0+a_0, -a_1+a_1, ...) = (0, 0, ...) = e$$

Komutativna grupa:

$$a + b = (a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...)$$

$$b + a = (b_0, b_1, ...) + (a_0, a_1, ...) = (b_0 + a_0, b_1 + a_1, ...)$$

Zbog komutativnosti elemenata iz prstena R vrijedi da su dobiveni izrazi jednaki.

Pokažimo sada da je $(R, \cdot)$ polugrupa:

Grupoid:

$$a \cdot b = (a_0, a_1, ...) \cdot (b_0, b_1, ...) = (a_0b_0, a_1b_0 + a_0b_1, a_2b_0 + a_1b_1 + a_0b_2, ...)$$

Ako je zadnji ne-nul element od a na indeksu k te zadnji ne-nul element od b na indeksu l, lako se provjeri da je zanji nenul element od $a \cdot b$ na indeksu $k + l$.

Polugrupa:

$(a \cdot b) \cdot c = f \cdot c = g$
$f_n = \sum_{k=0}^{n} a_k b_{n-k}$
$g_n = \sum_{i=0}^{n} f_i c_{n-i} = \sum_{i=0}^{n} (\sum_{k=0}^{i} a_k b_{i-k}) c_{n-i} = \sum_{i=0}^{n} \sum_{k=0}^{i} a_k b_{i-k} c_{n-i}$

$a \cdot (b \cdot c) = a \cdot e = d$
$e_n = \sum_{k=0}^{n} b_k c_{n-k}$
$d_n = \sum_{i=0}^{n} a_i e_{n-i} = \sum_{i=0}^{n} a_i (\sum_{k=0}^{n-i} b_k c_{n-i-k}) = \sum_{i=0}^{n} \sum_{k=0}^{n-i} a_i b_k c_{n-i-k}$

Zanima nas je li $g_n = d_n$.

$g_n = \sum_{i=0}^{n} \sum_{k=0}^{i} a_k b_{i-k} c_{n-i} = \sum_{k=0}^{n} \sum_{i=k}^{n} a_k b_{i-k} c_{n-i} = \sum_{k=0}^{n} \sum_{i=0}^{n-k} a_k b_i c_{n-(k+i)}$.
Za $k = i$ vrijedi da je $g_n = d_n$.

Pokažimo nadalje da vrijedi lijeva distributivnost množenja prema zbrajanju:

$$\begin{aligned} a \cdot (b + c) &= (a_0, a_1, ...) \cdot ((b_0, b_1, ...) + (c_0, c_1, ...)) \\ &= (a_0, a_1, ...) \cdot (b_0 + c_0, b_1 + c_1, ...) \\ &= (a_0 \cdot (b_0 + c_0), a_1 \cdot (b_0 + c_0) + a_0 \cdot (b_1 + c_1), ...) \\ &= (a_0 \cdot b_0 + a_0 \cdot c_0, a_1 \cdot b_0 + a_1 \cdot c_0 + a_0 \cdot b_1 + a_0 \cdot c_1, ...) \end{aligned}$$

$$\begin{aligned} a \cdot b + a \cdot c &= (a_0, a_1, ...) \cdot (b_0, b_1, ...) + (a_0, a_1, ...) \cdot (c_0, c_1, ...) \\ &= (a_0 \cdot b_0, a_1 \cdot b_0 + a_0 \cdot b_1, ...) + (a_0 \cdot c_0, a_1 \cdot c_0 + a_0 \cdot c_1, ...) \\ &= (a_0 \cdot b_0 + a_0 \cdot c_0, a_1 \cdot b_0 + a_0 \cdot b_1 + a_1 \cdot c_0 + a_0 \cdot c_1, ...) \end{aligned}$$

Zbog komutativnosti elemenata iz prstena R (s obzirom na operaciju $+$) vrijedi da su dobiveni izrazi jednaki, odnosno vrijedi: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Pokažimo da vrijedi i desna distributivnost množenja prema zbrajanju:

$$\begin{aligned} (a + b) \cdot c &= ((a_0, a_1, ...) + (b_0, b_1, ...)) \cdot (c_0, c_1, ...) \\ &= (a_0 + b_0, a_1 + b_1, ...) \cdot (c_0, c_1, ...) \\ &= ((a_0 + b_0) \cdot c_0, (a_1 + b_1) \cdot c_0 + (a_0 + b_0) \cdot c_1, ...) \\ &= (a_0 \cdot c_0 + b_0 \cdot c_0, a_1 \cdot c_0 + b_1 \cdot c_0 + a_0 \cdot c_1 + b_0 \cdot c_1, ...) \end{aligned}$$

$$\begin{aligned} a \cdot c + b \cdot c &= (a_0, a_1, ...) \cdot (c_0, c_1, ...) + (b_0, b_1, ...) \cdot (c_0, c_1, ...) \\ &= (a_0 \cdot c_0, a_1 \cdot c_0 + a_0 \cdot c_1, ...) + (b_0 \cdot c_0, b_1 \cdot c_0 + b_0 \cdot c_1, ...) \\ &= (a_0 \cdot c_0 + b_0 \cdot c_0, a_1 \cdot c_0 + a_0 \cdot c_1 + b_1 \cdot c_0 + b_0 \cdot c_1, ...) \end{aligned}$$

Isto kao i kod lijeve distributivnosti, zbog komutativnosti elemenata iz prstena R (s obzirom na operaciju $+$), vrijedi da su dobiveni izrazi jednaki, odnosno

vrijedi: $(a+b)\cdot c = a\cdot c + b\cdot c$.

(ii) • Neka je R komutativan prsten. Da bi $R[x]$ bio komutativan prsten, za a, b iz $R[x]$ mora vrijediti: $a\cdot b = b\cdot a$.

$$\begin{aligned} a\cdot b &= (a_0, a_1, a_2, ...)\cdot(b_0, b_1, b_2, ...) \\ &= (a_0\cdot b_0, a_1\cdot b_0 + a_0\cdot b_1, ...) \end{aligned}$$

$$\begin{aligned} b\cdot a &= (b_0, b_1, b_2, ...)\cdot(a_0, a_1, a_2, ...) \\ &= (b_0\cdot a_0, b_1\cdot a_0 + b_0\cdot a_1, ...) \end{aligned}$$

Zbog komutativnosti elemenata iz R sa operacijama + i $\cdot$ slijedi da su dobiveni izrazi jednaki po svim koordinatama.

• Neka je R prsten s jedinicom (označimo sa 1_R njegov neutralni element). Da bi $R[x]$ bio prsten s jedinicom, mora postojati jedinstveni $e \in R[x]$ takav da je $a\cdot e = e\cdot a = a$, za svaki $a \in R[x]$. Potražimo najprije $e \in R[x]$ takav da je $a\cdot e = a$.

$$\begin{aligned} a\cdot e = a &\iff (a_0, a_1, a_2, ...)\cdot(e_0, e_1, e_2, ...) = (a_0, a_1, a_2, ...) \\ &\iff (a_0\cdot e_0, a_1\cdot e_0 + a_0\cdot e_1, a_2\cdot e_0 + a_1\cdot e_1 + a_0\cdot e_2, ...) = (a_0, a_1, a_2, ...) \\ &\iff a_0\cdot e_0 = a_0 \ \&\ a_1\cdot e_0 + a_0\cdot e_1 = a_1 \ \&\ a_2\cdot e_0 + a_1\cdot e_1 + a_0\cdot e_2 = a_2 \ \&... \\ &\iff e_0 = 1_R \ \&\ e_1 = 0 \ \&\ e_2 = 0 \ \&\ ... \\ &\iff e = (1_R, 0, 0, ...) \end{aligned}$$

Analogno bi se pokazalo da je $e'\cdot a = a$ pri čemu je $e' = (1_R, 0, 0, ..)$.
Dakle, $e = e' = (1_R, 0, 0, ...)$ je neutralni element u $R[x]$.

• Za dokaz sljedeće tvrdnje trebat će nam lema:

Lema 2.1.3. Neka su $a = (a_0, a_1, ...), b = (b_0, b_1, ...) \in R[x]$ i neka je k (odnosno j) najmanji indeks takav da je $a_k \neq 0$ (odnosno $b_j \neq 0$). Tada vrijedi:

$$(a_0, a_1, ...)(b_0, b_1, ...) = \underbrace{(0, 0, ..., 0,}_{\text{k+j nula}} a_k b_j, a_{k+1} b_j + a_k b_{k+1}, ...).$$

Pokažimo sada sljedeću tvrdnju svođenjem na kontradikciju:

Početna tvrdnja glasi: Neka je R prsten bez djelitelja nule. Tada je $R[x]$ prsten bez djelitelja nule.
Pretpostavimo suprotno. Neka $R[x]$ nije prsten bez djelitelja nule, odnosno neka je R[x] prsten sa djeliteljima nule. To znači da postoje $a, b \in R[x]$ $a, b \neq 0$, takvi da je $ab = 0$. Neka je $a = (a_0, a_1, ...) \neq 0$ (odnosno $b = (b_0, b_1, ...) \neq 0$) takav da je k (j) najmanji indeks za koji je $a_k \neq 0$ ($b_j \neq 0$).
Promotrimo umnožak polinoma a i b.

$$\begin{aligned} a \cdot b &= (a_0, ..., a_k, ...) \cdot (b_0, ..., b_k, ...) \\ &= \underbrace{(0, 0, ..., 0}_{\substack{k+j \text{ nula} \\ \text{zbog Leme} \\ 2.1.3}} , a_k b_j, ...) \end{aligned}$$

Postavlja se pitanje čemu je jednak umnožak a_k i b_j ($a_k \neq 0, b_j \neq 0$). S obzirom da su a_k, b_j elementi prstena bez djelitelja nule, slijedi da je $a_k b_j \neq 0$. Dakle, kako je jedna koordinata različita od nule, slijedi da je ab različit od nule, što je kontradikcija s početnom pretpostavkom.

- Neka je R integralna domena, to jest neka je R prsten s jedinicom i prsten bez djelitelja nule. Tada je $R[x]$ prsten s jedinicom i prsten bez djelitelja nule (prethodno pokazano). Odnosno $R[x]$ je integralna domena.

(iii) Pokažimo da je funkcija r homomorfizam i injektivna.
Homomorfizam:

- $r(a + b) = (a + b, 0, 0, ...) = (a, 0, 0, ...) + (b, 0, 0, ...) = r(a) + r(b)$

- $r(a \cdot b) = (a \cdot b, 0, 0, ...) = (a, 0, 0, ...) \cdot (b, 0, 0, ...) = r(a) \cdot r(b)$

Injektivnost:
Neka su $a, b \in R$ takvi da $a \neq b$. Tada je $r(a) = (a, 0, 0, ...), r(b) = (b, 0, 0, ...)$. Kako je $a \neq b$ slijedi da je $r(a) \neq r(b)$.

■

Prsten $R[x]$ iz danog teorema zove se **prsten polinoma u jednoj varijabli** iznad prstena R i njegovi elementi zovu se polinomi.

Primjer 2.1.4. Prsten polinoma nad $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. △

Napomena 2.1.5. Označimo $(r, 0, 0, ...)$ sa r. Primijetimo da je onda

$$\begin{aligned} r \cdot (a_0, a_1, a_2, ...) &= (r, 0, 0, ...) \cdot (a_0, a_1, a_2, ...) \\ &= (r \cdot a_0, 0 \cdot a_1 + r \cdot a_0, 0 \cdot a_2 + 0 \cdot a_1 + r \cdot a_2, ..., \sum_{i=0}^{n} r_{n-i} a_i, ...) \\ &= (r \cdot a_0, r \cdot a_1, r \cdot a_2, ..., r \cdot a_n, ...) \end{aligned}$$

Analogno bi se dokazalo da je $(a_0, a_1, a_2, ...) \cdot r = (a_0 \cdot r, a_1 \cdot r, a_2 \cdot r, ...)$.

△

Napomena 2.1.6. Ako je (1_R) neutralni element za množenje u R, onda je $(1_R, 0, 0, ...)$ neutralni element za množenje u $R[x]$. △

Sljedeći teorem govori o potenciranju elementa x gdje je x iz prstena s jedinicom te o zapisu ne-nul polinoma f iz prstena s jedinicom.

Teorem 2.1.7. Neka je R prsten s jedinicom i označimo sa x element $(0, 1_R, 0, 0, ...)$ iz $R[x]$. Tada vrijedi:

(i) $x^n = (0, 0, 0, ..., 1_R, 0, ...)$, gdje je 1_R na $(n+1)$ koordinati.

(ii) Ako je $r \in R$, onda za svaki $n \geq 0, rx^n = x^n r = (0, 0, ..., 0, r, 0, ...)$, gdje se r nalazi na $(n+1)$ koordinati.

(iii) Za svaki ne-nul polinom f iz $R[x]$ postoji $n \in \mathbb{N}$ i elementi $a_0, ..., a_n \in R$ takvi da je $f = a_0x^0 + a_1x^1 + a_2x^2 + ... + a_nx^n$. Broj n i elementi a_i su jedinstveni u smislu da, kad bi postojali $b_0, ..., b_m$ takvi da je $f = b_0x^0 + b_1x^1 + b_2x^2 + ... + b_mx^m (b_i \in R)$, to bi povlačilo da je $m \geq n$ i da je $a_i = b_i$ za $1 < i \leq n$ i $b_i = 0$ za $n < i \leq m$.

Dokaz.

(i) Dokažimo matematičkom indukcijom.

Baza indukcije: $x^1 = x = (0, 1_R, 0, ...)$.
Pretpostavimo da vrijedi da je $x^n = (0, 0, 0, ..., 1_R, 0, ...)$, gdje je 1_R na $(n+1)$ koodinati.
Pokažimo da tvrdnja vrijedi za potenciju $n+1$.

$$x^{n+1} = x^n \cdot x = \underbrace{(0, 0, 0, ...,}_{\text{n nula iz pretp.}} 1_R, 0, ...) \cdot \underbrace{(0,}_{\text{1 nula}} 1_R, 0, ...) = \underbrace{(0, 0, ..., 0,}_{\substack{\text{n+1 nula} \\ \text{zbog Leme} \\ \text{2.1.3.}}} 1_R, 0, ...)$$

Dakle, 1_R se nalazi na $(n+2)$ koordinati.

Dokazali smo da tvrdnja vrijedi za $n = 1$ i da iz pretpostavke da vrijedi za n slijedi da tvrdnja vrijedi za $n+1$, pa zadana tvrdnja prema aksiomu matematičke indukcije vrijedi za svaki prirodan broj n.

(ii) $$r \cdot x^n = r \cdot \underbrace{(0, 0, 0, ...,}_{\text{n nula}} 1_R, 0, ...) \overset{\text{(Nap. 2.1.5.)}}{=} (0, 0, ..., r, 0, ...)$$

$$x^n \cdot r = \underbrace{(0, 0, 0, ...,}_{\text{n nula}} 1_R, 0, ...) \cdot r \overset{\text{(Nap. 2.1.5.)}}{=} (0, 0, ..., r, 0, ...)$$

(iii) Neka je $f = (f_0, f_1, f_2, ...) \in R[x]$ i neka je k najveći indeks takav da je $f_k \neq 0$. Tada je

$$\begin{aligned} f &= (f_0, f_1, ..., f_k, 0, 0, ...) \\ &= (f_0, 0, 0, ...) + (0, f_1, 0, 0, ...) + ... + (0, ..., 0, f_k, 0, 0, ...) \\ &= f_0(1, 0, 0, ...) + f_1(0, 1, 0, ...) + ... + f_k(0, ..., 0, 1, ...) \\ &= f_0x^0 + f_1x^1 + ... + f_kx^k \end{aligned}$$

Za $n = k$ i $a_i = f_i$ slijedi da je $f = a_0x^0 + ... + a_nx^n$.
Pretpostavimo najprije da je $m \geq n$. Tada je

$$\begin{aligned} &a_0x^0 + ... + a_nx^n = b_0x^0 + ... + b_mx^m \\ &a_0x^0 - b_0x^0 + a_1x^1 - b_1x^1 + ... + a_nx^n - b_nx^n - b_{n+1}x^{n+1} - ... - b_mx^m = 0 \\ &(a_0 - b_0)x^0 + (a_1 - b_1)x^1 + ... + (a_n - b_n)x^n - b_{n+1}x^{n+1} - ... - b_mx^m = 0 \\ &(a_0 - b_0, 0, ...) + (0, a_1 - b_1, 0, ...) + ... + (0, ..., 0, a_n - b_n, 0, ...) + \\ &+ (0, ..., 0, -b_{n+1}, 0, ...) + ...(0, ..., 0, -b_m, 0, ...) = (0, 0, ...). \end{aligned}$$

Tada slijedi:

$$\begin{array}{rcl} a_0 - b_0 = 0 & & a_0 = b_0 \\ a_1 - b_1 = 0 & & a_1 = b_1 \\ \vdots & & \vdots \\ a_n - b_n = 0 & \Longleftrightarrow & a_n = b_n \\ -b_{n+1} = 0 & & b_{n+1} = 0 \\ \vdots & & \vdots \\ -b_m = 0 & & b_m = 0. \end{array}$$

Pretpostavimo sada da je $m < n$. Tada bismo analognim postupkom došli do zaključka da je $a_{m+1} = 0,\ ...,\ a_n = 0,$ što je kontradikcija s početnom pretpostavkom da je n najveći indeks takav da je $a_n \neq 0$.

■

Do sada smo promatrali prsten polinoma jedne varijable, a sada ćemo promatrati prstene polinoma više varijabli. Najprije ćemo iskazati teorem analogan teoremu 2.1.2.

Teorem 2.1.8. Neka je R prsten. Označimo sa $R[x_1, ..., x_n]$ skup svih funkcija $f : \mathbb{N}^n \to R$ takvih da je $f(u) \neq 0$ za najviše konačno mnogo elementata u od $\mathbb{N}^n$. Tada vrijedi:

(i) $R[x_1, ..., x_n]$ je prsten sa zbrajanjem $(f + g)(u) = f(u) + g(u)$
i množenjem $(fg)(u) = \sum_{v \leq u,\ v \in \mathbb{N}^n} f(v)g(u - v)$
gdje su $f, g \in R[x_1, ..., x_n]$ i $u \in \mathbb{N}^n$

(ii) Ako je R komutativan (analogno prsten s jedinicom ili prsten bez djelitelja nule ili integralna domena), onda je i $R[x_1, ..., x_n]$

(iii) Funkcija $R \to R[x_1, ..., x_n]$ zadana preslikavanjem $r \mapsto f_r$, gdje je $f_r(0, ..., 0) = r$ i $f(u) = 0$ za sve $(0, 0, ..., 0) \neq u \in \mathbb{N}^n$ je monomorfizam prstena.

Prsten $R[x_1, ..., x_n]$ zovemo **prsten polinoma u** n **varijabli** iznad R.

Teorem 2.1.9. Neka je R prsten s jedinicom i neka je n prirodan broj. Za svaki $i = 1, 2, ..., n$ neka je $x_i \in R[x_1, ..., x_n]$ definiran kao $x_i(\epsilon_i) = 1_R$ i $x_i(u) = 0$ za $u \neq \epsilon_i$ Tada vrijedi:

(i) Za svaki $k \in \mathbb{N}, x_i^k(k\epsilon_i) = 1_R$ i $x_i^k(u) = 0$ za $u \neq k\epsilon_i$

(ii) Za svaki $(k_1, ..., k_n) \in \mathbb{N}^n, x_1^{k_1} x_2^{k_2} ... x_n^{k_n}(k_1\epsilon_1 + ... + k_n\epsilon_n) = 1_R$ i $x_1^{k_1} x_2^{k_2} ... x_n^{k_n}(u) = 0$ za $u \neq k_1\epsilon_1 + ... + k_n\epsilon_n$

(iii) $x_i^s x_j^t = x_j^t x_i^s$ za sve $s, t \in \mathbb{N}$ i sve $i, j \in 1, ..., n$

(iv) $x_i^t r = r x_i^t$ za sve $r \in R$ i sve $t \in \mathbb{N}$

(v) Za sve polinome f iz $R[a_1, ..., x_n]$ postoje jedinstveni elementi $a_{k_1,...,k_n} \in R$ indeksirani sa svim $(k_1, ...k_n) \in \mathbb{N}^n$ takvih da su različiti od nula za najviše

konačno indeksa $(k_1, ..., k_n) \in \mathbb{N}^n$ takvih da je
$f = \sum a_{k_1,...,k_n} x_1^{k_1} ... x_n^{k_n}$ gdje je suma za sve $(k_1, ..., k_n) \in \mathbb{N}^n$.

2.2 Prsten formalnih redova

U ovom potpoglavlju uočit ćemo vezu između prstena polinoma u jednoj varijabli i prstena formalnih redova u jednoj varijabli te ćemo pokazati postojanje i svojstva invertibilnih elemenata u prstenu formalnih redova.

Propozicija 2.2.1. Neka je R prsten i označimo sa $R[[x]]$ skup svih nizova elemenata od $R(a_0, a_1, a_2, ...)$. Tada vrijedi:

(i) $R[[x]]$ je prsten sa zbrajanjem

$$(a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...)$$

i množenjem

$$(a_0, a_1, ...) \cdot (b_0, b_1, ...) = (c_0, c_1, ...)$$

gdje je

$$\begin{aligned} c_n &= \sum_{i=0}^{n} a_{n-i} b_i \\ &= \sum_{k+j=n} a_k b_j. \end{aligned}$$

(ii) Prsten polinoma $R[x]$ je potprsten od $R[[x]]$.

(iii) Ako je R komutativni prsten (analogno: prsten s jedinicom ili prsten bez djelitelja nule ili integralna domena), onda je i $R[[x]]$.

Prsten $R[[x]]$ nazivamo **prsten formalnih redova** nad prstenom R. Njegovi elementi zovu se formalni redovi.
Ako je R prsten s jedinicom, onda je $x = (0, 1_R, 0, ...) \in R[[x]]$.

Lako je uočiti da je $x^i r = rx^i$, za svaki $r \in R$ i $i \in \mathbb{N}$.
Ako je $(a_0, a_1, ...) \in R[[x]]$, onda za svaki n vrijedi da je $(a_0, a_1, a_2, ..., a_n, 0, 0, ...)$ polinom, gdje je $(a_0, a_1, a_2, ..., a_n, 0, 0, ...) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ (prema Teoremu 2.1.7.).
Formalne redove $(a_0, a_1, ...) \in R[[x]]$ označavat ćemo slično kao i polinome, $\sum_{i=0}^{\infty} a_i x^i$.
Elemente a_i zovemo **koeficijentima** te posebno, a_0 nazivamo **konstantnim članom**.

Propozicija 2.2.2. Neka je R prsten s jedinicom i neka je $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$. Tada vrijedi:

(i) f ima inverz u $R[[x]]$, ako i samo ako njegov konstantni član a_0 ima inverz u R.

(ii) Ako je a_0 ireducibilan u R, onda je f ireducibilan u $R[[x]]$.

Dokaz.

(i) $\boxed{\Longleftarrow}$

Pretpostavimo da konstantni član a_0 formalnog reda $f \in R[[x]]$ ima inverz u R. Ako postoji $g = \sum b_i x^i \in R[[x]]$ takav da je $fg = 1_{R[[x]]}$ onda vrijedi:

$$
\begin{aligned}
fg &= 1_{R[[x]]} \\
(a_0, a_1, ..., a_n, ...) \cdot (b_0, b_1, ..., b_n, ...) &= (1_R, 0, 0, ...) \\
(a_0b_0, a_1b_0 + a_0b_1, ..., a_nb_0 + a_{n-1}b_1 + ... + a_0b_n, ...) &= (1_R, 0, ..., 0, ...)
\end{aligned}
$$

$$
\begin{aligned}
&\iff \\
a_0b_0 &= 1_R \\
a_1b_0 + a_0b_1 &= 0 \\
&\vdots \\
a_nb_0 + a_{n-1}b_1 + ... + a_0b_n &= 0 \\
&\vdots
\end{aligned}
$$

$$
\begin{aligned}
&\iff \\
b_0 &= a_0^{-1} \\
b_1 &= a_0^{-1}(-a_1b_0) \\
&\vdots \\
b_n &= a_0^{-1}(-a_nb_0 - ... - a_1b_{n-1}) \\
&\vdots
\end{aligned}
$$

S obzirom da a_0 ima inverz, svi članovi od g se mogu izračunati rekurzivno. Dakle, takav g postoji te vrijedi: $fg = 1_{R[[x]]} \in R[[x]]$. Analogno možemo pokazati da postoji h takav da je $hf = 1_{R[[x]]} \in R[[x]]$. S obzirom da $h = h1_{R[[x]]} = h(fg) = (hf)g = 1_{R[[x]]}g = g$ vrijedi da je g obostrani inverz od f.

$\boxed{\Longrightarrow}$

Neka je $g = \sum b_i x^i \in R[[x]]$ inverzni element od f. Tada vrijedi: $fg = gf = 1_{R[[x]]} \in R[[x]]$, to jest
$(a_0, a_1, ...)(b_0, b_1, ...) = (b_0, b_1, ...)(a_0, a_1, ...) = (1_R, 0, ...)$
$(a_0b_0, a_1b_0 + a_0b_1, ...) = (b_0a_0, b_1a_0 + b_0a_1, ...) = (1_R, 0, ...)$

iz čega slijedi $a_0b_0 = b_0a_0 = 1_R$ što znači da a_0 ima inverz u R.

(ii) S obzirom da je a_0 ireducibilan, vrijedi da je $0 \neq a_0 \notin R^\times$ te da $a_0 = g_0h_0$ gdje $g_0 \in R^\times$ i / ili $h_0 \in R^\times$. Kako je $f = (a_0, a_1, a_2, ...)$ slijedi da je $f \neq 0$ (jer je konstantni član različit od nule) te $f \notin R^\times$ jer mu konstantni član nije invertibilan. Trebamo još pokazati da je $f = gh$ gdje je $g \in R^\times$ i / ili $h \in R^\times$. S obzirom da je $a_0 = g_0h_0$, slijedi da je $g \in R^\times$ i / ili $h \in R^\times$.

■

Napomena 2.2.3. Ako je $f \in R[[x]]$ polinom s invertibilnim (odnosno ireducibilnim) konstantnim članom, onda f nije nužno invertibilan (odnosno ireducibilan) polinom u $R[x]$. △

Korolar 2.2.4. Ako je R tijelo, onda su invertibilni elementi iz $R[[x]]$ točno oni formalni redovi čiji je konstantni član različit od nule. Glavni ideal (x) sastoji se točno od neinvertibilnih elemenata iz $R[[x]]$ i on je jedinstveni maksimalni ideal od $R[[x]]$. Dakle, ako je R polje, onda je $R[[x]]$ lokalni prsten.

Dokaz. S obzirom na to da je R tijelo, slijedi da svaki element iz R (osim nule) ima inverz. Kako postojanje inverza u $R[[x]]$ ovisi o slobodnom koeficijentu formalnog reda, slijedi da je formalni red invertibilan ako i samo ako mu je slobodni član bilo koji element iz R osim nule.

Pokažimo najprije da je x iz centra od $R[[x]]$. Tada mora vrijediti: $xr = rx, \forall r \in R[[x]]$.

$$\begin{aligned} xr &= (0, 1_R, 0, ...)(r_0, r_1, r_2, ...) \\ &= (0, 1_R \cdot r_0, 1_R \cdot r_1, ...) \\ &= (0, r_0, r_1, ...) \\ &= (0, r_0 \cdot 1_R, r_1 \cdot 1_R, ...) \\ &= (r_0, r_1, r_2, ...)(0, 1_R, 0, ...) = rx. \end{aligned}$$

Nadalje, prema Teoremu 1.2.19. slijedi da je glavni ideal (x) jednak:

$$\begin{aligned}(x) = xR[[x]] &= \{xf, f \in R[[x]]\} \\ &= \{x \cdot (a_0, a_1, a_2, ...),\ \forall i\ a_i \in R\} \\ &= \{(0, 1_R, 0, ...) \cdot (a_0, a_1, a_2, ...),\ \forall i\ a_i \in R\} \\ &= \{(0, a_0, a_1, ...),\ \forall i\ a_i \in R\}.\end{aligned}$$

Vidimo da svaki element glavnog ideala (x) ima konstantni član jednak nuli, što znači da glavni ideal (x) sadrži točno sve neinvertibilne elemente.

Pokažimo da je (x) maksimalni ideal.
Pretpostavimo da postoji $J \trianglelefteq R[[x]]$ takav da je $(x) \subset J \subset R[[x]]$.
Tada postoji a takav da je $a \in J$ i $a \notin (x)$.
Za svaki takav a vrijedi da je $a_0 \neq 0$ što znači da je a invertibilan. S obzirom da je J ideal, za svaki $x \in R[[x]]$ vrijedi $ax \in J$. Slijedi da je $aa^{-1} = 1_{R[[x]]} \in J$. S obzirom da je $1_R \in J$ te s obzirom da je J ideal, slijedi da za svaki $p \in R[[x]]$ vrijedi da je $p \cdot 1_{R[[x]]} = p \in J$. Odnosno, $J = R[[x]]$.

Pokažimo da je (x) jedinstveni maksimalni ideal.
S obzirom da svaki ideal $I, I \neq R[[x]]$ sadrži samo neinvertibilne elemente slijedi da je svaki ideal $I \neq R[[x]] \subset (x)$. Dakle, (x) je jedinstveni maksimalni ideal.

Dakle, pokazali smo da ako je R tijelo, onda $R[[x]]$ sadrži jedinstveni maksimalni ideal. Nadalje, ako je R komutativno tijelo (polje), onda je prema Propoziciji 2.2.1. $R[[x]]$ komutativni prsten s jedinicom koji sadrži jedinstveni maksimalni ideal, odnosno, $R[[x]]$ je lokalni prsten. ■

Teorem 2.2.5. Neka je $R[[x]]$ prsten formalnih redova nad prstenom R. Skup $A = \{(0, a_1, a_2...) : a_i \in R\}$ tvori ideal.

Dokaz. $A \trianglelefteq R[[x]] \iff$

1. $A \leq R[[x]]$
   Neka su $a, b \in A$. Tada vrijedi:

$a - b = (0, a_1, a_2, ...) - (0, b_1, b_2, ...) = (0, a_1 - b_1, a_2 - b_2, ...) \in A.$
$ab = (0, a_1, a_2, ...)(0, b_1, b_2, ...) = (0, 0, a_1 b_1, ...) \in A.$

2. $\forall r \in R[[x]], \forall a \in A$ vrijedi $ar \in A$ (odnosno $ra \in A$).
   Neka je $a \in A, r \in R[[x]]$. Tada vrijedi:
   $ar = (0, a_1, a_2, ...)(r_0, r_1, r_2, ...) = (0, a_1 r_0, ...) \in A.$
   $ra = (r_0, r_1, r_2, ...)(0, a_1, a_2, ...) = (0, r_0 a_1, ...) \in A.$

   Dakle, $A \trianglelefteq R[[x]]$.

■

Bibliografija

[1] K. Horvatić, *Linearna algebra*, Matematički odjel PMF-a Sveučilišta u Zagrebu i Hrvatsko matematičko društvo, Zagreb, 1995.

[2] T. W. Hungerford, *Algebra, Graduate Texts in Mathematics vol. 73*, Springer, 2003.

[3] B. Pavković, D. Veljan, *Elementarna matematika 1*, Tehnička knjiga, Zagreb, 1992.

[4] B. Širola, *Algebarske strukture*, dostupno na `https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf` (lipanj, 2018.)

Sažetak

Cilj ovog diplomskog rada (koji smo podijelili u dva poglavlja) je konstruirati prsten polinoma i formalnih redova u jednoj i više varijabli te proučiti njihova osnovna svojstva.

U prvom poglavlju prikazali smo glavne rezultate iz teorije prstena – definicije jednostavnijih algebarskih struktura (grupoida, polugrupa, monoida, grupa) koje smo postupno gradili do osnovne strukture kojom se bavimo u radu – prstena. Osim definicije i primjera prstena, u poglavlju smo još definirali i neke bogatije strukture kao što su tijelo i polje.

U drugom poglavlju definirali smo osnovne operacije (zbrajanje i množenje) u prstenu polinoma jedne i više varijabli te u formalnim redovima jedne varijable s ciljem da bismo pokazali da skupovi polinoma i formalnih redova sa definiranim operacijama tvore prsten. Nadalje, proučavali smo međusobne odnose između prstena polinoma i formalnih redova, kao i odnose sa skupovima iz kojih potječu njihovi koeficijenti. Na kraju poglavlja prikazali smo uvjete postojanja i neka svojstva invertibilnih elemenata u prstenu formalnih redova.

Summary

Goal of this graduate thesis is to construct a ring of polynomials (and formal power series) in one and more indeterminates over a ring R and to study their main properties. Thesis is divided into two chapters.
In the first chapter we show main concepts from ring theory - definitions of algebraic structures (groupoid, semigroup, monoid, group) that we use to construct the ring. Beside the definition and examples of rings, in this chapter we define some structures like division ring and field.
In second chapter we define operations (addition and multiplication) in polynomial ring and in formal power series ring (with one and more indeterminates). For those structures and operations, we show that they form a ring. We study relations between ring of polynomials and its superset ring of formal power series, as well as relation with ring from which their coefitients came from. In the end of second chapter we show conditions for existence of a unit and some of the properties of units in formal power series.

Životopis

Zovem se Judita Janković. Rođena sam 07.11.1991. u Čakovcu. Osnovnu školu pohađala sam u Osnovnoj školi Petra Zrinskog u Šenkovcu, a srednju u Gimnaziji Josipa Slavenskog u Čakovcu. Preddiplomski studij nastavničkog smjera matematike na Matematičkom odsjeku Prirodoslovnog-matematičko fakulteta upisala sam 2010./2011. godinu, a završila 2013./2014. Nakon toga, 2014./2015. upisala sam diplomski studij nastavničkog smjera matematike, koji završavam 2017./2018.